REMARKS

Reconsideration of the above-indicated patent application, as amended, is respectfully requested. The present amendment is responsive to the Office Action mailed November 2, 2004. Claims 1-24 have been rejected. Accordingly, amended claims, new claims and supporting remarks are hereby presented that particularly point out and distinctly claim the subject matter that applicant regards as the invention. No new matter has been added.

THE REJECTIONS UNDER 35 U.S.C § 112

Claims 2 and 4 had been rejected under Section 112, second paragraph, as being indefinite because the limitation "the step of initiating" lacked sufficient antecedent basis. Claim 2 has been amended to overcome this rejection, claim 4 has been canceled.

THE REJECTIONS UNDER 35 U.S.C § 103

Claims 1-24 had been rejected under Section 103(a) as being unpatentable over Newton in "Encyclopedia of Cryptology." This rejection is respectfully traversed, particularly as applied to the amended and new claims.

The Examiner states that Newton discloses loading into memory a plurality of keys simultaneously to decrypt a previous data frame. The basis for this statement is that Newton discloses using a previously decrypted letter as a key to decrypting the next letter, so that the key is "loaded" while decrypting the previous "data frame" or letter. The Examiner admits that Newton fails to disclose using such a method on a computer system, but takes official notice that encryption algorithms are commonly used on computer systems.

By contrast, the claims of the present invention as now presented, recite loading into memory a first decryption key comprising a first plurality of key values while key values are being read out from the memory. An aspect of the present invention is that read and write operations of the key memory can be performed at the same time. In accordance with an aspect of the present invention, claims 1-3 recite that the loading and reading out steps occur simultaneously, and claims 25-50 recite that the loading step starts before the reading out has completed. Claims 25, 30, 35 and 40 recite that the keys are read out to initialize a table while

the loading is being performed. Claims 27, 29, 32, 34, 37, 39, 42, 44 and 45 recite that a second key, different from the first key, is being loaded into the memory while the first key is being read out.

An aspect of the present invention improves performance by loading a key for the next encryption (or decryption) operation before the previous encryption (or decryption) operation has completed. Thus, while one set of key values are being read from the memory for performing a first encryption (or decryption) operation, the key for the next encryption (or decryption) operation is loaded into the memory. Furthermore, the keys for the next encryption (or decryption) operation, which is different from the keys already loaded, are loaded while the first process is performing other decryption tasks. For example, keys can be loaded into the memory while keys are read from memory to initialize a table, such as an S-box table. Keys can also be loaded into memory for the next operation while the table (*e.g.*, S-box table) is being scrambled and/or while a data frame is being encrypted or decrypted. By contrast, the cited prior only teaches using a previous decrypted letter to decrypt the next letter.

Thus, for the reasons cited prior art does not teach suggest or show the claims as now presented. Applicant respectfully requests withdrawal of this rejection.

In view of the foregoing it is respectfully submitted that the present claims, as currently amended, distinguish over the prior art. A notice to that effect is earnestly solicited. If the Examiner believes there are any further matters, which need to be discussed in order to expedite the prosecution of the present application, the Examiner is invited to contact the undersigned.

Respectfully submitted,

TUCKER ELLIS & WEST LLP

Date: 12-29-2004

Larry B. Donovan
Registration No. 47,230
1150 Huntington Building
925 Euclid Avenue
Cleveland, Ohio 44115-1475
Customer No. 23380
(216) 696-3864 (phone)
(216) 592-5009 (fax)